IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (Currently Amended) An information reproducing apparatus, comprising:

a hardware secure module having a tamper resistant module structure and storing ~~that stores a first~~ information related to secure software~~, wherein the secure module can not be accessed from outside~~;

a memory that stores the secure software ~~a second information, wherein the memory can be accessed from outside~~;

a falsification checking unit that is loaded on the hardware secure module, wherein the falsification checking unit reads the ~~second information~~ secure software from the memory by direct access without using an operation system, compares the ~~second information~~ secure software with the ~~first~~ information in the hardware secure module, and checks ~~a falsification of~~ whether the ~~second information~~ secure software is falsified based on a result of the comparison; and

a processor that executes ~~reproducing unit playing-back~~ the ~~second information~~ secure software when a result of the check by the falsification checking unit is that the ~~second information~~ secure software is not falsified.

2. (Currently Amended) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads all of the ~~second information~~ secure software.

3. (Currently Amended) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads a part of the ~~second information~~ secure software.

4. (Currently Amended) The information reproducing apparatus according to claim 1, wherein the falsification checking unit performs the comparison of the ~~first~~ information and the ~~second information~~ secure software using a checksum method.

5. (Cancelled).

6. (Currently Amended) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads the ~~second information~~ secure software from the memory on an irregular basis.

7. (Currently Amended) The information reproducing apparatus according to claim 1, further comprising:

~~an~~ a storing unit that is loaded on the hardware secure module and that updates the ~~second information~~ secure software in the memory using a direct access method.

8. (Currently Amended) The information reproducing apparatus according to claim 7, wherein the storing unit updates the ~~second information~~ secure software on an irregular basis.

·9. (Currently Amended) The information reproducing apparatus according to claim 7, wherein the storing unit updates a part of the ~~second information~~ secure software.

10. (Currently Amended) The information reproducing apparatus according to claim 7, wherein the falsification checking unit reads the ~~second information~~ secure software updated by the storing unit.

11. (Currently Amended) The information reproducing apparatus according to claim 7, wherein when the ~~second information~~ secure software is updated, the storing unit changes over the ~~second information~~ secure software which has been updated.

12. (Currently Amended) The information reproducing apparatus according to claim 7, wherein the storing unit stores encrypted data in the memory ~~the second information~~ after encryption using a key that exists in the hardware secure module.

13. (Currently Amended) The information reproducing apparatus according to claim 1, further comprising:

a key managing unit that is loaded ~~on~~ in the hardware secure module, wherein the key managing unit holds a key used to encrypt or decode ~~the second information~~ data stored in the memory, and the key managing unit outputs the key, if the falsification checking unit does not detect a falsification.

14. (Original) The information reproducing apparatus according to claim 13, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

15. (Previously Presented) The information reproducing apparatus according to claim 13, wherein the key managing unit changes the key each time the key managing unit outputs the key.

16. (Previously Presented) The information reproducing apparatus according to claim 13, wherein when the falsification checking unit detects a falsification, the key managing unit does not output the key.

17. (Currently Amended) The information reproducing apparatus according to claim 1, further comprising:

a writing unit that is loaded ~~on~~ in the hardware secure module, wherein the writing unit writes a secret information within the hardware secure module into the memory ~~as the second information~~ using the direct access method, wherein

the falsification checking unit checks falsification of the ~~second information~~ secure software based on response information corresponding to the secret information.

18. (Previously Presented) The information reproducing apparatus according to claim 17, wherein the secret information is stored in a controlled memory space, wherein

the controlled memory space is such that a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time.

19. (Currently Amended) The information reproducing apparatus according to claim 1, wherein the ~~second information is~~ secure software has a function of decoding encrypted MPEG data.

20. (Currently Amended) An information reproducing method comprising:

reading ~~second information~~ secure software stored in a memory using direct access method without using an operating system, by a hardware secure module having a tamper resistant module structure ~~storing~~ which stores ~~a first~~ information related to the secure software~~,~~

~~wherein the secure module can not be accessed from outside, and the memory can be accessed from outside using a direct access method~~;

checking falsification by comparing the ~~second information~~ secure software with the ~~first~~ information, and ~~checking a falsification of~~ determining whether the ~~second information~~ secure software is falsified based on a result of the comparison; and

~~playing-back the second information~~ executing the secure software when ~~a~~ result of ~~checking falsification~~ determining is that the ~~second information~~ secure software is not falsified.

21. (Currently Amended) A hardware secure module mounted to an information reproducing apparatus and having a tamper resistant module structure, comprising:

a reading unit that reads a ~~second information~~ secure software from a memory mounted to ~~a~~ the information reproducing apparatus by direct access~~, wherein the memory can be accessed from outside~~ without using an operating system; and

a falsification checking unit that compares the ~~second information~~ secure software with ~~a first~~ information related to the secure software stored in the hardware secure module, and checks a falsification of the ~~second information~~ secure software based on a result of the comparison, wherein if the result of the comparison shows that the ~~second information~~ secure software is not falsified the ~~second information~~ secure software is ~~played-back~~ executed by the information reproducing apparatus.

22. (Currently Amended) The hardware secure module according to claim 21, wherein the reading unit reads all of the ~~second information~~ secure software.

23. (Currently Amended) The hardware secure module according to claim 21, wherein the reading unit reads a part of the ~~second information~~ secure software.

24. (Currently Amended) The hardware secure module according to claim 21, wherein the falsification checking unit performs the comparison of the ~~first~~ information and the ~~second information~~ secure software using a checksum method.

25. (Cancelled).

26. (Currently Amended) The hardware secure module according to claim 21, wherein the reading unit reads the ~~second information~~ secure software from the memory on an

irregular basis.

27. (Currently Amended) The hardware secure module according to claim 21, further comprising:

a storing unit that stores the ~~second information~~ secure software in the memory using a direct access method.

28. (Currently Amended) The hardware secure module according to claim 27, wherein the storing unit updates the ~~second information~~ secure software on an irregular basis.

29. (Currently Amended) The hardware secure module according to claim 27, wherein the storing unit updates a part of the ~~second information~~ secure software.

30. (Currently Amended) The hardware secure module according to claim 27, wherein the falsification checking unit reads the ~~second information~~ secure software updated by the storing unit.

31. (Currently Amended) The hardware secure module according to claim 27, wherein when the ~~second information~~ secure software is updated, the storing unit changes over the ~~second information~~ secure software which has been updated.

32. (Currently Amended) The hardware secure module according to claim 27, wherein the storing unit stores ~~the second information~~ encrypted data in the memory after encryption using a key that exists in the secure module.

33. (Currently Amended) The hardware secure module according to claim 21, further comprising:

a key managing unit that holds a key used to encrypt or decode ~~the second information~~ data stored in the memory, and the key managing unit outputs the key, if the falsification checking unit does not detect a falsification.

34. (Currently Amended) The hardware secure module according to claim 33, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

35. (Currently Amended) The hardware secure module according to claim 33, wherein the key managing unit changes the key each time the key managing unit outputs the key.

36. (Currently Amended) The hardware secure module according to claim 33, wherein when the falsification checking unit detects a falsification, the key managing unit does not output the key.

37. (Currently Amended) The hardware secure module according to claim 21, further comprising:

a writing unit that writes a secret information within the secure module into the memory ~~as the second information~~ using the direct access method, wherein

the falsification checking unit ~~checks~~ determines falsification of the ~~second information~~ based on response information corresponding to the secret information.

38. (Currently Amended) The hardware secure module according to claim 37, wherein the secret information is stored in a controlled memory space, wherein the controlled memory space is such that a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time.

39. (Currently Amended) The hardware secure module according to claim 21, wherein the ~~second information is~~ secure software has a function of decoding encrypted MPEG data.

40. (Currently Amended) A recording medium that records a program for causing a hardware secure module mounted to an information reproducing apparatus to execute a process, the process comprising:

reading ~~a second information~~ secure software using a direct access method and without using an operating system, by the hardware secure module having a tamper resistant module structure storing ~~stored in a memory mounted to the information reproducing apparatus, wherein the secure module stores a first~~ information related to the secure software~~, and the secure module can not be accessed from outside, and the memory can be accessed from outside using a direct access method~~;

checking falsification by comparing the ~~second information~~ secure software with the first information, and determining a falsification of the ~~second information~~ secure software based on a result of the comparison; and

executing the secure software ~~playing-back the second information~~ when the result of the comparison is that the ~~second information~~ secure software is not falsified.

41. (Currently Amended) A method of a reproducing verified information, comprising:

~~playing-back second information~~ executing secure software that is stored in a memory accessible ~~from outside~~ to an information reproducing apparatus using a direct access method, if comparison of the ~~second information~~ secure software with ~~first~~ information related to the secure software stored in a hardware secure module having a tamper resistant module structure inaccessible from outside, indicates that the ~~second information~~ secure software is not falsified.